DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of the Army organizational name (APMS Sub Organization name).

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (F&MWRC)

2. Name of Information Technology (IT) System (APMS System name).

Standard Non-Appropriated Fund (NAF) Automated Contracting System (SNACS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9998

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository DITPR)).

586

5. IT Investment (OMB Circular A-1 1) Unique Identifier (if applicable)

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215-2b CFSC Commercial Entertainment Transaction Records (July 26, 2001, 66 FR 39027). The system notice will be updated specific to this data collection.

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

10 U.S.C. 3013, Secretary of the Army;
26 U.S.C. 6041, Information at Source;
Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities;
Army Regulation 215-4, Nonappropriated Fund Contracting;
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);
DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR);
E.O. 9397 (SSN).

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

SNACS is an automated procurement application that is Web based and hosted on one of four Morale, Welfare and Recreation (MWR) Application Service Provider (ASP) sites. The SNACS system allows the users to allocate funding and approve the spending. The users must be approved by management to perform these tasks. The workflow application provides for creation, routing, approval and contract award for any Non Appropriated Fund procurement. The NAF Contracting Directorate on behalf of MWR owns the system. The system is one of several applications hosted on the Application Service Provider (ASP). The boundaries are the ASP; there are no interconnections with other systems. The systems are located in Ft. Sam Houston, TX, Rock Island, IL, Continuity of Operations Plans (COOP) and Ft. Humphries, Korea. All Oracle databases are auto archived approximately every 20 minutes. This creates a backup restorable to twenty minutes ago at any time. This data is stored at the ASP COOP site at Rock Island Arsenal.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Employee information is used to create a user account for access to, and accountability in, the procurement system. The information collected is name, office address, office email address, office telephone. The information collected comes directly from the employee or their supervisor using a SNACS new user form. The system provides user id, and individuals create their own passwords.

Vendor information collected is name, vendor email address, telephone, address, tax number and form W-2 Wage and Tax Statement information.

11. Describe how the information will be collected (e.g. via the Web, via paper-based collection).

Using a SNACS new user form, a trained and approved administrator collects employee information that is required to create a user account and to allow the worker access to the approved level of security within the procurement system. The new user form is electronic and is transmitted over the Army e-mail system; the form is destroyed after data is entered into SNACS.

Vendor information is collected and entered into the system by our buyers. A trained and approved buyer collects information directly from the vendor that desires to do business with our department.

12. Describe the requirement and why the information in identifiable form is to be collected Describe how the information in identifiable form will be used (e.g., to verify existing data, (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

Personally identifiable information (PII) on employees is used to create a user account in SNACS. The user account provides access to, and accountability for, actions taken in the system. All document actions can be linked directly to the responsible user. The properly identified and credentialed user then uses SNACS to solicit, purchase, account and pay for products and services rendered to the Army Morale Welfare & Recreation program.

PII on vendors is used to contact vendors, negotiate contracts and send solicitations and awards to vendors for product purchase.

13. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation.

14. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Data can be shared among contracting officers, site application administrators, installation application administrators and system users. The data is not shared with any other system.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

15. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Before any PII is collected, individuals are provided a privacy act advisory statement.

16. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Individuals are provided a privacy act advisory statement which explains the requirement and authority to collect the information.

17. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

The data is stored within a secure datacenter on a secure Army Installation with all protections afforded by Army and Defense Information System Agency (DISA) security infrastructure. The datacenter has passed the required security measures tests required for Information Assurance System Accreditation and has a full Authority to Operate. Additionally, the system is built on redundancy with a full COOP site.

All personnel accessing the SNACS system have received a favorable National Agency Check. The users include 1) active duty military, 2) Federal civil service personnel in the contracting department who have a need to know in order to perform official government duties and 3) administration personnel who have been cleared to perform system maintenance.

Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role.

Each specific application in the system may further restrict access via application-unique permission controls. Currently, only system users and service liaisons (and their authorized contract users) have the capability to connect to the system.

With the exception of systems administrators, information assurance security officers and software maintenance personnel, users fall into non-sensitive Information Technology (IT) Category III (non-privileged) positions as designated in DoD Directive 8500.1. Persons in IT Category-III positions require a National Agency Check, Entrance National Agency Check, or National Agency Check with Inquiries. All system administrators, information assurance and software maintenance personnel are in non-sensitive IT Category-I (privileged) positions. Persons in IT Category-I positions require a Single Scope Background Investigation (SSBI).

Information is made available to users through the application or Enterprise server. Each authorized user must enter an appropriate User/Identification and Password before being authorized access to the resources.

There is weekly monitoring and immediate disabling of accounts with easily guessed passwords, daily notification of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). Partners are provided information through regularly scheduled file transfers accomplished via file transfer protocol or email across the RSN or Non-classified but Sensitive Internet. Protocol Router Network

(NIPRNET). Files transferred across the Internet/NIPRNET are encrypted using a Virtual Private Network (VPN) or Advanced Encryption Standard (AES) 256-bit encryption. All as designated in DoD Directive 8500.1.

18. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A systems notice currently exists and will be either amended to be more descriptive of this business practice or an entirely new system notice will be developed.

19. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

20. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The SNACS program privacy data is for official use only. The PIA may be published in its entirety.